



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/683,874	10/09/2003	Yung Chang Liang	TRNDP012	7893
22434	7590	03/19/2007		
BEYER WEAVER LLP P.O. BOX 70250 OAKLAND, CA 94612-0250			EXAMINER DEBNATH, SUMAN	
			ART UNIT 2135	PAPER NUMBER

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/19/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	Application No. 10/683,874	Applicant(s) LIANG ET AL.	
	Examiner Suman Debnath	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 10/09/2003.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>03/01/2005 &amp; 04/11/2005</u> . | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. Claims 1-20 are pending in this application.

#### ***Claim Objections***

2. Claim 15 is objected to because the claim is dependent on "claim a2" in line 1. It is assumed that applicant intended to claim dependency of claim 12. Appropriate correction is required.

#### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-6 and 11-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yanovsky (Patent No.: US 7,010,807 B1) in view of Suorsa et al. (Pub. No.: US 2002/0156894 A1), hereinafter Suorsa.

5. As to claim 1, Yanovsky discloses in a distributed network having a number of server computers and associated client devices, method of enforcing an anti-virus security policy (FIG. 1, abstract), comprising: querying each of the client devices to determine if each of the client devices has an appropriate anti-virus software installed (column 4, lines 25-30 and lines 59-63); identifying those queried client devices not

having the appropriate anti-virus software as target client devices (column 4, lines 35-40 and 63-67, "...checks the version number against the current version number"); and installing the appropriate anti-virus software to all target client devices (column 4, lines 40-45 and column 5, lines 5-11).

Yanovsky doesn't explicitly disclose locking all communications channels of the target client devices to an anti-virus software installation server. However, Suorsa discloses locking all communications channels of the target client devices to a anti-virus software installation server ([0009], [0070]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Yanovsky by locking all communications channels of the target client devices to a anti-virus software installation server as taught by Suorsa in order to "ensure that the agents are not overburdened" (Suorsa). Furthermore one would be motivated to do so to make the installation software faster.

6. As to claim 2, Yanovsky discloses a method further comprising: connecting a new client device to the network (column4, lines 25-37); and installing the appropriate anti-virus software in the newly connected client device (column 4, lines 40-45 and column 5, lines 5-11). Yanovsky doesn't explicitly disclose locking all communications channels of the client device to a anti-virus software installation server. However, Suorsa discloses locking all communications channels of the client device to a anti-virus software installation server ([0009], [0070]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Yanovsky by locking all communications channels of the client device to a anti-virus software installation server as taught by Suorsa in order to “ensure that the agents are not overburdened” (Suorsa). Furthermore one would be motivated to do so to make the installation software faster.

7. As to claim 3, Yanovsky discloses a method wherein the appropriate anti-virus software is determined by a set of policies contained in an operating procedures and policy file (column 3, lines 55-65).

8. As to claim 4, Yanovsky discloses a method further comprising: posting a notification that the target client devices and the newly connected client devices are prevented from communicating with other systems in the network until such time as the appropriate anti-virus software has been installed therein (column 3, lines 60-67 and column 4, lines 35-45, which describes denying access for any host devices that fails to meet the policy and grant access after installation of software).

9. As to claim 5, Yanovsky discloses a method further comprising: once the appropriate anti-virus software has been installed in the target client devices or the newly connected client devices, can communicate with the other devices of network (column 4, lines 60-67 and column 5, lines 1-21, which describes granting access to the host devices after updating the host devices with current version of software

components). Yanovsky doesn't explicitly disclose relinquishing the lock on the communication channels for client devices. However, Suorsa discloses relinquishing the lock on the communication channels for client devices (e.g., claim 11).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Yanovsky by relinquishing the lock on the communication channels for client devices as taught by Suorsa in order to free up the resources.

10. As to claim 6, Yanovsky doesn't explicitly disclose wherein the newly connected client device is a visitor client device. However, Suorsa discloses a visitor client device ([0014], "remote agents").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Yanovsky by supporting a visitor client device as taught by Suorsa in order to provide support to the external clients with updated software component.

11. As to claim 11, Yanovsky discloses in a distributed network having a number of server computers and associated client devices, computer program product for enforcing an anti-virus security policy (abstract), comprising: computer code for querying each of the client devices to determine if each of the client devices has an appropriate anti-virus software installed (column 4, lines 25-30 and lines 59-63); computer code for identifying those queried client devices not having the appropriate

anti-virus software as target client devices (column 4, lines 35-40 and 63-67); computer code for installing the appropriate anti-virus software to all target client devices (column 4, lines 40-45 and column 5, lines 5-11); and computer readable medium for storing the computer code (FIG. 1).

Yanovsky doesn't explicitly disclose computer code for locking all communications channels of the target client devices to an anti-virus software installation server. However, Suorsa discloses computer code for locking all communications channels of the target client devices to a anti-virus software installation server ([0009], [0070]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Yanovsky by including computer code for locking all communications channels of the target client devices to an anti-virus software installation server as taught by Suorsa in order to "ensure that the agents are not overburdened" (Suorsa). Furthermore one would be motivated to do so to make the installation software faster.

12. As to claim 12, Yanovsky discloses computer program product further comprising: computer code for connecting a new client device to the network (column 4, lines 25-37); and computer code for installing the appropriate anti-virus software in the newly connected client device (column 4, lines 40-45 and column 5, lines 5-11). Yanovsky doesn't explicitly disclose computer code for locking all communications channels of the client device to a anti-virus software installation server. However,

Suorsa disclose computer code for locking all communications channels of the client device to a anti-virus software installation server ([0009], [0070]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Yanovsky by including computer code for locking all communications channels of the client device to a anti-virus software installation server as taught by Suorsa in order to "ensure that the agents are not overburdened" (Suorsa). Furthermore one would be motivated to do so to make the installation software faster.

13. As to claim 13, Yanovsky discloses computer program product wherein the appropriate anti-virus software is determined by a set of policies contained in an operating procedures and policy file (column 3, lines 55-65).

14. As to claim 14, Yanovsky discloses computer program product further comprising: computer code for posting a notification that the target client devices and the newly connected client devices are prevented from communicating with other systems in the network until such time as the appropriate anti-virus software has been installed therein (column 3, lines 60-67 and column 4, lines 35-45).

15. As to claim 15, Yanovsky discloses computer program product further comprising: computer code for once the appropriate anti-virus software has been installed in the target client devices or the newly connected client devices, can



communicate with the other devices of network (column 4, lines 60-67 and column 5, lines 1-21). Yanovsky doesn't explicitly disclose computer code for relinquishing the lock on the communication channels for the client devices. However, Suorsa discloses computer code for relinquishing the lock on the communication channels for the client devices (e.g., claim 11).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Yanovsky by including computer code for relinquishing the lock on the communication channels for the client devices as taught by Suorsa in order to free up the resources.

16. As to claim 16, Yanovsky discloses computer program product wherein the newly connected client device is a visitor client device (column 4, lines 25-45, "host device").

17. Claims 7-10 and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yanovsky in view of Suorsa and further in view of Herrmann et al. (Pub. No.: US 2003/0055994 A1), hereinafter Herrmann.

18. As to claim 7, Yanovsky discloses a method further comprising: determining whether or not the visitor client device is compliant with the appropriate anti-virus software (column 4, lines 25-45 and lines 52-67). Neither Yanovsky nor Suorsa explicitly disclose granting a temporary credential for use by the visitor client device when it is determined that the visitor client device is compliant with the appropriate anti-virus

Art Unit: 2135

software. However, Herrmann discloses granting a temporary credential for use by the visitor client device when it is determined that the visitor client device is compliant with the appropriate anti-virus software ([0075], [0077], "session").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Yanovsky and Suorsa by granting a temporary credential for use by the visitor client device when it is determined that the visitor client device is compliant with the appropriate anti-virus software as taught by Herrmann in order to "ensure that all machines connected to a server or a network, including client computers that are joining (e.g., remotely connecting to) a network, are using specified anti-virus products to protect against infiltration by viruses" (Herrmann).

19. As to claim 8, Neither Yanovsky nor Suorsa explicitly disclose a method further comprising: periodically determining validity of the credential. However, Herrmann discloses a method further comprising: periodically determining validity of the credential ("...subsequently reevaluate the decision to permit access", e.g., [0077]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Yanovsky and Suorsa by periodically determining validity of the credential as taught by Herrmann in order to maintain the integrity of access control of network devices.

20. As to claim 9, Neither Yanovsky nor Suorsa explicitly disclose a method further comprising: invalidating the credential when it is determined to not be valid. However, Herrmann discloses invalidating the credential when it is determined to not be valid ([0077], e.g., "session", "restrict one or more client devices").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Yanovsky and Suorsa by invalidating the credential when it is determined to not be valid as taught by Herrmann in order to maintain the integrity of access control of network devices.

21. As to claim 10, Neither Yanovsky nor Suorsa explicitly disclose a method wherein the credential not valid after a period of time as determined by the granting. However, Herrmann discloses a method wherein the credential not valid after a period of time as determined by the granting ("...a defined frequency interval", e.g., [0077]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Yanovsky and Suorsa by a method wherein the credential not valid after a period of time as determined by the granting as taught by Herrmann in order to maintain the integrity of access control of network devices.

22. As to claim 17, Yanovsky discloses computer program product further comprising: computer code for determining whether or not the visitor client device is compliant with the appropriate anti-virus software (column 4, lines 25-45 and lines 52-

67). Neither Yanovsky nor Suorsa explicitly disclose computer code for granting a temporary credential for use by the visitor client device when it is determined that the visitor client device is compliant with the appropriate anti-virus software. However, Herrmann discloses computer code for granting a temporary credential for use by the visitor client device when it is determined that the visitor client device is compliant with the appropriate anti-virus software ([0075], [0077], "session").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Yanovsky and Suorsa by granting a temporary credential for use by the visitor client device when it is determined that the visitor client device is compliant with the appropriate anti-virus software as taught by Herrmann in order to "ensure that all machines connected to a server or a network, including client computers that are joining (e.g., remotely connecting to) a network, are using specified anti-virus products to protect against infiltration by viruses" (Herrmann).

23. As to claim 18, Neither Yanovsky nor Suorsa explicitly disclose computer program product further comprising: computer code for periodically determining validity of the credential. However, Herrmann discloses computer code for periodically determining validity of the credential ("...subsequently reevaluate the decision to permit access", e.g., [0077]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Yanovsky and Suorsa by

Art Unit: 2135

periodically determining validity of the credential as taught by Herrmann in order to maintain the integrity of access control of network devices.

24. As to claim 19, Neither Yanovsky nor Suorsa explicitly disclose computer program product further comprising: invalidating the credential when it is determined to not be valid. However, Herrmann discloses invalidating the credential when it is determined to not be valid ([0077], e.g., "session", "restrict one or more client devices").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Yanovsky and Suorsa by invalidating the credential when it is determined to not be valid as taught by Herrmann in order to maintain the integrity of access control of network devices.

25. As to claim 20, Neither Yanovsky nor Suorsa explicitly disclose computer program product wherein the credential not valid after a period of time as determined by the granting. Herrmann discloses computer program product wherein the credential not valid after a period of time as determined by the granting ("...a defined frequency interval", e.g., [0077]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Yanovsky and Suorsa by a method wherein the credential not valid after a period of time as determined by the granting as taught by Herrmann in order to maintain the integrity of access control of network devices.

### ***Conclusion***

26. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See accompanying PTO 892.

Kouznetsov et al. (Patent Number: US 6,892,241 B2) discloses a method wherein the anti-virus scanning software is updated utilizing the network.

Freund et al. (Pub. No.: US 2003/0055962 A1) discloses a method wherein security module looks for the appropriate code to verify anti-virus program on client machine.

Tanaka et al. (Patent No. 5,548,725) discloses a method for data communication in looked mode.

27. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

Art Unit: 2135

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SD  
SD

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100